IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION,

Plaintiff,

v.

NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*,

Defendants.

Hon. T. S. Ellis, III

Civil Action No.
15-cv-00662-TSE

PLAINTIFF'S MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION TO COMPEL DISCOVERY RESPONSES AND DEPOSITION TESTIMONY

Deborah A. Jeon (Bar No. 06905)
David R. Rocah (Bar No. 27315)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838
jeon@aclu-md.org

Patrick Toomey (pro hac vice)
Ashley Gorski (pro hac vice)
Jonathan Hafetz (pro hac vice)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ptoomey@aclu.org

Alex Abdo (pro hac vice)
Jameel Jaffer (pro hac vice)
KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY
475 Riverside Drive, Suite 302
New York, NY 10115
Phone: (646) 745-8500
alex.abdo@knightcolumbia.org

Counsel for Plaintiff

Table of Contents

Table of Authorities

Cases

Statutes

Rules

Other Authorities

Introduction

In accordance with Federal Rule of Civil Procedure 37, Plaintiff Wikimedia Foundation ("Wikimedia") respectfully submits this motion to compel responses to certain interrogatories, requests for admission, and requests for production propounded on Defendants. Wikimedia also seeks to compel Rule 30(b)(6) deposition testimony on related topics from the NSA.

After the Fourth Circuit held that Wikimedia had plausibly alleged the copying and review of its communications by the NSA, *see Wikimedia Found. v. NSA*, 857 F.3d 193 (4th Cir. 2017), Wikimedia requested information from the government regarding the NSA's Upstream surveillance of Internet traffic on U.S. soil. While the government has provided certain information that was already publicly available, it has refused to provide any meaningful response to requests seeking information (1) confirming that some of Wikimedia's trillion-plus international communications each year are copied and reviewed by the NSA; (2) defining key terms that the government has used to describe the operation of Upstream surveillance to the public; and (3) regarding the scope and breadth of Upstream surveillance. In short, although the government has previously made extensive disclosures about this surveillance program in public testimony, public reports, public statements, and publicly released opinions of the Foreign Intelligence Surveillance Court ("FISC"), it has refused to disclose a single additional fact about Upstream surveillance in response to Wikimedia's requests.

Throughout its responses, the government has instead asserted a sweeping exception to its discovery obligations, relying on: the common law state secrets privilege derived from *United States v. Reynolds*, 345 U.S. 1 (1953); Section 102A of the National Security Act of 1947, 50 U.S.C. § 3024(i); and Section 6 of the National Security Agency Act of 1959 ("NSAA"), 50 U.S.C. § 3605(a). *See* Toomey Decl., Ex. 9–19 (Defendants' objections and responses).

Each of those assertions fails as a matter of law. The detailed discovery and in camera review procedures of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 *et seq.*, regulate access to the information Wikimedia seeks. Those procedures apply "whenever any motion or request is made . . . to discover or obtain applications or orders or other materials relating to electronic surveillance," *id.* § 1806(f), and they therefore displace the common law state secrets privilege. And, in any event, the state secrets privilege would not prevent disclosure of the information Plaintiff seeks.

Nor does the National Security Act bar disclosure of the information Wikimedia seeks. The provision cited by Defendants, 50 U.S.C. § 3024(i), does not establish a litigation privilege. It cannot be invoked to refuse to disclose otherwise discoverable information. The general language of Section 6 of the NSAA, 50 U.S.C. § 3605(a), which was enacted prior to the more specific language of FISA, 50 U.S.C. § 1806(f), does not prevent disclosure either.

Wikimedia requests that the Court apply FISA's statutory discovery procedures, 50 U.S.C. § 1806(f), and compel the government to disclose its discovery responses to the Court, so that the Court may review the information in camera to make the necessary factual and legal determinations concerning jurisdiction. That is the process the district court has adhered to in *Jewel v. NSA*, No. 08-cv-4373 (N.D. Cal.), and it is the same process the Court should apply in this case. *See, e.g.*, Order, *Jewel v. NSA*, No. 08-cv-4373 (February 19, 2016) (ECF No. 340) ("The procedural mechanism under 50 U.S.C. section 1806(f) of FISA serves to alleviate the risk of disclosure of state secret information."); Minute Order, *Jewel v. NSA*, No. 08-cv-4373 (May 19, 2017) (ECF No. 356). In the alternative, if the Court concludes that Congress did not displace the state secrets privilege through FISA, the Court should hold that the government's invocations of privilege fail to justify the secrecy it demands here.

I. Summary of the evidence sought by Wikimedia

The evidence Wikimedia has sought concerning the surveillance of its communications falls into three principal categories. *See also* Section I.D *infra*; Toomey Decl., Ex. 1 (listing the requests at issue).

A. Direct evidence that Wikimedia has been surveilled

First, Wikimedia has sought direct evidence confirming that some of its trillion-plus international communications each year are surveilled. Specifically, Wikimedia has sought documents and admissions establishing that the NSA has copied, reviewed, and retained some of Wikimedia's communication in the course of Upstream surveillance. *See* Pl. Requests for Production No. 23, 24 (Toomey Decl., Ex. 1); Pl. Requests for Admission No. 34–36 (same). For example, Wikimedia has asked Defendants to admit:

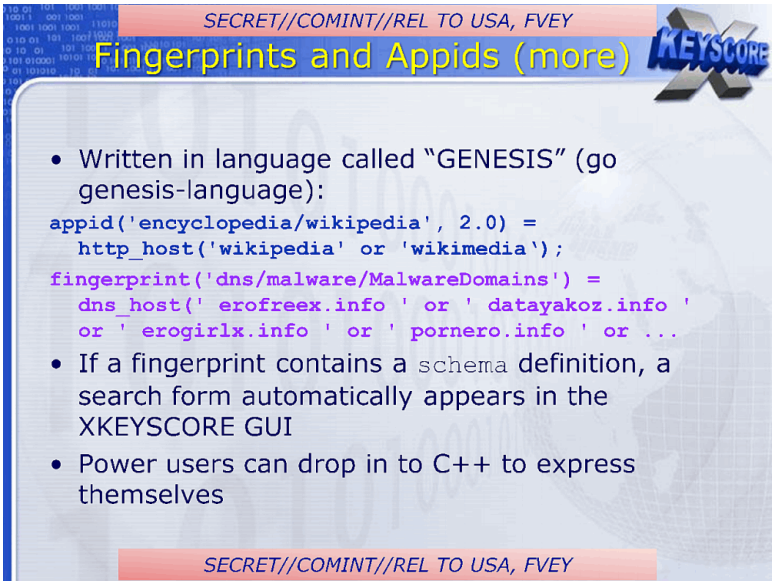
> **Request for Admission No. 35**: Admit that, in conducting Upstream surveillance, the NSA has REVIEWED the content of at least one WIKIMEDIA INTERNET COMMUNICATION.

Likewise, Wikimedia has asked Defendants to produce:

> **Request for Production No. 23**: Any INTERNET COMMUNICATION of WIKIMEDIA that any DEFENDANT INTERACTED WITH in connection with Upstream surveillance.

Wikimedia has also sought admissions confirming the authenticity of NSA documents describing the surveillance of Wikimedia. *See* Pl. Requests for Admission No. 16–18, 19–21 (Toomey Decl., Ex. 1). In particular, Wikimedia has asked Defendants to admit the authenticity of two NSA slides that show an express interest in surveilling Wikimedia's communications. Wikimedia's Request for Admission No. 16 asks Defendants to confirm the authenticity of a slide describing the NSA's interest in surveilling HTTP communications to and from Wikipedia websites:

Similarly, Wikimedia's Request for Admission No. 19 asks Defendants to confirm the authenticity of another NSA slide, which describes computer code for identifying intercepted "wikipedia" and "wikimedia" communications:



B. Key terms used in describing Upstream surveillance to the public

Second, Wikimedia has sought basic information concerning the government's prior public disclosures about Upstream surveillance. This evidence is relevant to Wikimedia's showing that, given the government's own official descriptions of how it conducts this

surveillance on the Internet backbone, as well as the immense volume and global distribution of Wikimedia's Internet communications, some of Wikimedia's communications are necessarily copied and reviewed in the course of Upstream surveillance. *See, e.g.*, Am. Compl. ¶¶ 49–51, 60–66, 88 (ECF No. 72); *Wikimedia Found.*, 857 F.3d at 210–11.

Accordingly, Wikimedia has sought information and documents defining key terms that the government and the FISC have used to describe the operation of Upstream surveillance to the public. For example, in an opinion released by Defendants, the FISC describes how Upstream surveillance is conducted at one or more "international Internet link[s]," citing the government's submissions to the court. [*Redacted*], No. [Redacted], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011). Because the term "international Internet link" describes the points at which the NSA is monitoring communications on the Internet backbone, Wikimedia propounded the following interrogatory:

> **Interrogatory No. 1:** DESCRIBE YOUR understanding of the definition of the term "international Internet link" as used by the Foreign Intelligence Surveillance Court in describing Upstream surveillance, *see* [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011), and provide all information supporting that understanding.

Pl. Interrogatory No. 1 (Toomey Decl., Ex. 1) (as modified). Despite their past public disclosures, Defendants have refused to explain the meaning of this term. *See* NSA Resp. to Pl. Interrogatory No. 1 (Toomey Decl., Ex. 11) (refusing to respond).

The same pattern holds across a wide swath of Plaintiff's requests: Defendants have refused to provide any meaningful explanation of other key terms the government has used to describe the operation of Upstream surveillance. *See, e.g.*, NSA Resp. to Pl. Interrogatories No. 5–9 (Toomey Decl., Ex. 11).

C. Evidence concerning the scope and breadth of Upstream surveillance

Third, Wikimedia has sought information concerning the scope and breadth of Upstream surveillance, again based in significant part on the government's existing public disclosures. These requests, too, will corroborate Wikimedia's showing that some of its trillion-plus international communications each year are copied and reviewed as the NSA monitors traffic on major Internet backbone circuits.

For example, Wikimedia has sought admissions that, in the course of Upstream surveillance, the NSA engages in the bulk copying and bulk review of communications in transit on the Internet backbone:

> **Request for Admission No. 7**: Admit that, in conducting Upstream surveillance, the NSA COPIES INTERNET COMMUNICATIONS in BULK that are in transit on the INTERNET BACKBONE.
>
> **Request for Admission No. 8**: Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS in BULK that are in transit on the INTERNET BACKBONE.

Defendants refused to respond at all to the first request, and provided a non-responsive answer to the second. *See* NSA Resp. to Pl. Requests for Admissions No. 7–8 (Toomey Decl., Ex. 9) (stating that "certain" Internet transactions "are filtered . . . then screened"). But Wikimedia's requests for admission are predicated on the government's official disclosures, which make clear that the NSA is copying and reviewing in bulk the international text-based communications on the circuits it is monitoring. *See* Privacy and Civil Liberties Oversight Board ("PCLOB"), *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* 122 (2014), https://perma.cc/J3DZ-62HL ("PCLOB Report") ("Digital communications like email, however, enable one, as a technological matter, to examine the contents of all transmissions passing through collection devices and acquire those, for instance, that contain a tasked selector

anywhere within them."); [*Redacted*], 2011 WL 10945618, at *10, *15; *cf.* David Kris & J. Douglas Wilson, National Security Investigations & Prosecutions § 17.5 (2015) ("NSA's machines scan the contents of *all* of the communications passing through the collection point, and the presence of the selector or other signature that justifies the collection is not known until *after* the scanning is complete.") (emphasis in original).

Wikimedia has also sought information about the overall breadth of Upstream surveillance, including: the number and percentage of circuits the NSA has monitored, *see* Pl. Requests for Production No. 13 & 16 (Toomey Decl., Ex. 1); and the amount of Internet traffic subject to Upstream surveillance, *see* Pl. Interrogatory No. 18 (same). While Wikimedia's international communications are so great in volume and so widely dispersed that they transit each of the circuits the NSA is monitoring, information about the breadth of the surveillance will rebut any claim that the NSA is monitoring just a small handful of circuits or just a miniscule amount of traffic. For example, Wikimedia has sought admissions confirming the authenticity of documents showing that the NSA is monitoring "many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States." *See* Pl. Requests for Admission No. 25 & Ex. D (Toomey Decl., Ex. 2). Similarly, Wikimedia has sought confirmation of the authenticity of a document showing that the NSA monitors large quantities of circuits at individual international chokepoints:

(TS//SI//NF) FAIRVIEW: CLIFFSIDE Site - Collection Resumes After ~5 Months
By [redacted] on 2011-08-23 0805

(TS//SI//NF) On 5 Aug 2011, collection of DNR and DNI traffic at the FAIRVIEW CLIFFSIDE trans-pacific cable site resumed, after being down for approximately five months. Collection operations at CLIFFSIDE had been down since 11 March 2011, due to the cable damage as a result of the earthquake off of the coast of Japan. The initial damage assessment showed the loss of collection of 275 E1 DNR circuits and 55 DNI circuits. Since the cable was repaired and returned to service (5 Aug), FAIRVIEW operations has tasked 205 E1 DNR circuits and 37 DNI circuits for collection. Enviornmental survey continues to compare the old enviornment footprint to the new environment footprint and FAIRVIEW operations will continue to task collection for all new and restored circuits.

POC: [redacted] S35333, [redacted] (FAIRVIEW Collection Manager)

See Pl. Request for Admission No. 39 & Ex. A (Toomey Decl., Ex. 4).

D. The discovery requests at issue

Because Defendants invoked the state secrets privilege and purported statutory privileges so broadly—to cover even basic admissions drawn from the government's prior public disclosures—a significant number of Plaintiff's requests are at issue in this motion. For ease of reference, the full set of requests at issue is identified below. These requests, as modified by Wikimedia following the parties' meet-and-confer discussions, are set out more fully in the chart provided in Exhibit 1 of the Toomey Declaration.

(1) Information regarding the surveillance of Wikimedia's communications:

a. Pl. Requests for Admission No. 16–18, 19–21, 34–36

b. Pl. Requests for Production No. 23–24

(2) Key terms used in describing Upstream surveillance to the public:

a. Pl. Interrogatories No. 1–9

b. Pl. Requests for Production No. 21–22

(3) Information regarding the scope and breadth of Upstream surveillance:

- Pl. Requests for Admission No. 6–10, 13–15, 25–30, 37–40
- Pl. Interrogatories No. 9, 14–20
- Pl. Requests for Production No. 10, 13–16, 18, 21–22

For each of the requests above, Defendants have refused to respond altogether or have provided an incomplete—and often non-responsive—answer, citing the state secrets privilege, 50 U.S.C. § 3024(i), and 50 U.S.C. § 3605(a). *See* Toomey Decl., Ex. 9–19 (Defendants' responses and objections). At times, Defendants have also asserted various other objections. *See* Section III *infra*.

(4) Illustrative Documents

For the Court's convenience, Wikimedia is also providing a list of illustrative documents, encompassed within the requests above, for which it seeks to compel disclosure. Some of these documents have been disclosed with significant redactions; others are simply identified on Defendants' privilege logs. Because Defendants have provided only limited information about the responsive records they are withholding—and, in some instances, have refused even to confirm or deny the existence of responsive documents—these are not the sum total of the documents Wikimedia is seeking.[1] Rather, based on the information currently available, Wikimedia identifies these examples for the Court:

a. Classified Declaration of Adm. Michael S. Rogers filed in *Jewel v. NSA*, No. 08-cv-4373 (N.D. Cal. Feb. 16, 2018), describing the locations on the Internet backbone where Upstream surveillance is conducted. *See* NSA Privilege Log No. 4 (Toomey Decl., Ex. 20).

b. Documents identifying circuits on which the NSA has conducted Upstream

[1] For example, Defendants have refused to confirm or deny the existence of Wikimedia-related documents responsive to Plaintiff's Requests for Production No. 23 and 24, *see* Toomey Decl., Ex. 13 (NSA responses and objections), and have provided only limited information about the contents of fully withheld documents in their privilege logs, *see* Toomey Decl., Ex. 20–22.

surveillance. *See* NSA Privilege Log No. 5 (Toomey Decl., Ex. 20).

c. PowerPoint presentation containing information about Upstream infrastructure. *See* NSA Privilege Log No. 7 (Toomey Decl., Ex. 20)

d. Document prepared by counsel in connection with *Jewel v. NSA*, No. 08-cv-4373 (N.D. Cal.), containing the locations on the Internet backbone where Upstream surveillance is conducted. *See* NSA Privilege Log No. 6. (Toomey Decl., Ex. 20).[2]

e. June 1, 2011 FISC Submission (Toomey Decl., Ex. 25).

f. June 28, 2011 FISC Submission (Toomey Decl., Ex. 26).

g. October 3, 2011 FISC Opinion (Toomey Decl., Ex. 27).

h. September 20, 2012 FISC Opinion (Toomey Decl., Ex. 28).

i. April 26, 2017 FISC Opinion (Toomey Decl., Ex. 29).

j. 2009 NSA Targeting Procedures. *See* Ex. E to Pl. Requests for Admission (Toomey Decl., Ex. 2); *see also* NSA Privilege Log No. 19 (Toomey Decl., Ex. 20).

k. 2014 NSA Targeting Procedures (Toomey Decl., Ex. 30)

E. Deposition testimony

Wikimedia also moves to compel deposition testimony from the NSA pursuant to Federal Rule of Civil Procedure 30(b)(6) on a related set of topics concerning Upstream surveillance. Pl. Dep. Notice (Toomey Decl., Ex. 23). As with its responses to the discovery requests above, the NSA seeks to limit its testimony on the basis of the state secrets privilege and purported statutory privileges, 50 U.S.C. § 3024(i) and 50 U.S.C. § 3605(a). NSA Dep. Objs. (Toomey Decl., Ex. 24). For the reasons explained below, Wikimedia requests that the Court employ FISA's in

[2] Defendants identified this document in response to Wikimedia's requests for documents "sufficient to show" the number of international Internet links or chokepoints where the NSA conducts Upstream surveillance. Pl. Requests for Production No. 15, 16 (Toomey Decl., Ex. 1). The NSA, however, has asserted attorney-client and work-product privilege over its contents. NSA Privilege Log (Toomey Decl., Ex. 20). If the NSA possesses other documents that would satisfy Wikimedia's requests, and that would not be subject to these claims of privilege, Wikimedia requests that the Court order the NSA to identify those documents.

camera review procedures, *see* 50 U.S.C. § 1806(f), to address any information that Defendants seek to withhold in response to deposition questions. *See* Section IV *infra*.

II. FISA's in camera review procedures govern the discovery Wikimedia seeks.

A. FISA's discovery provision, 50 U.S.C. § 1806(f), regulates access to the information Wikimedia seeks.

In 1978, Congress enacted FISA to govern surveillance conducted for foreign intelligence purposes. It did so after years of in-depth congressional investigation by a task force known as the Church Committee, which revealed that the Executive Branch had for decades engaged in widespread warrantless surveillance of United States citizens. Congress's express purpose in enacting FISA was to create a comprehensive statutory regime to prevent future misuse of electronic surveillance by the Executive. *See, e.g.*, Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, Book II: Intelligence Activities & the Rights of Americans, S. Rep. No. 94-755, at 289 (1976) ("[I]ntelligence activities have undermined the constitutional rights of citizens and . . . they have done so primarily because checks and balances designed by the framers of the Constitution to assure accountability have not been applied."); S. Rep. No. 95-604, pt. 1, at 7 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908 ("This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused.").

To further that goal, Congress enacted a detailed provision that governs discovery related to electronic surveillance. It reads in relevant part:

> [W]henever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States . . . to discover or obtain applications or orders or other materials relating to electronic surveillance . . . the United States district court . . . shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials

> relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

50 U.S.C. § 1806(f).

Section 1806(f) of FISA governs Wikimedia's motion to compel. First, Wikimedia is an "aggrieved person" within the meaning of FISA. FISA defines "aggrieved person" to include any "person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). Wikimedia has put forth detailed and specific allegations of the NSA's surveillance of its communications. *See* Am. Compl. The Fourth Circuit has held that those allegations plausibly establish the surveillance of Wikimedia's communications and, for that reason, establish Wikimedia's standing on a motion to dismiss. *Wikimedia Found.*, 857 F.3d at 209, 211 (Plaintiff's "allegations [are] sufficient to make plausible the conclusion that the NSA is intercepting, copying, and reviewing at least some of Wikimedia's communications."). Accordingly, Wikimedia has more than demonstrated that it is an "aggrieved person" for purposes of FISA. *See In re NSA Telecomms. Records Litig.*, 595 F. Supp. 2d 1077, 1085–89 (N.D. Cal. 2009) (holding that "plaintiffs have alleged enough to plead 'aggrieved person' status so as to proceed to the next step in proceedings under FISA's sections 1806(f)").

Second, Wikimedia has requested and is now moving to compel the disclosure of information it seeks pursuant to "any . . . rule of the United States," namely, the Federal Rules of Civil Procedure. 50 U.S.C. § 1806(f).

Third, Wikimedia is moving to compel the disclosure of "materials relating to electronic surveillance." *Id*. Each of the categories of information sought, *see* Section I *supra*, bears on whether the NSA is intercepting, copying, and reviewing Wikimedia's international Internet

communications in the course of Upstream surveillance. That is precisely the sort of information whose discovery is regulated by FISA's discovery procedures.

FISA gives the government two options in responding to Wikimedia's discovery requests for information relating to electronic surveillance. If the Attorney General files an affidavit stating that disclosure of the information sought would harm the national security of the United States, then the government must disclose the information requested to this Court, 50 U.S.C. § 1806(f), which "shall . . . review in camera and ex parte" the information to determine the lawfulness of the surveillance challenged. The Court may also order disclosure to Wikimedia "under appropriate security procedures and protective orders . . . where such disclosure is necessary to make an accurate determination of the legality of the surveillance." *Id.* If, on the other hand, the government does not submit such an affidavit from the Attorney General, disclosure of the requested information to Wikimedia is mandatory. S. Rep. No. 95-701, at 63 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4032 ("If no such assertion is made, the committee envisions . . . mandatory disclosure . . . ."); *see also* H.R. Rep. No. 95-1720, at 31–32 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048, 4060–61.

B. FISA's statutory discovery provision displaces the state secrets privilege.

FISA's discovery provision, 50 U.S.C. § 1806(f), displace the state secrets privilege with regard to information relating to electronic surveillance. A statute of Congress abrogates a federal common law rule, such as the state secrets privilege,[3] if it "'speak[s] directly' to the question addressed by the common law." *United States v. Texas*, 507 U.S. 529, 534 (1993); *see*

[3] *See, e.g.*, *Gen. Dynamics Corp. v. United States*, 563 U.S. 478, 491 (2011) (noting that the state secrets opinion issued therein is "a common-law opinion, which, after the fashion of the common law, is subject to further refinement"); *In re United States*, 872 F.2d 472, 474 (D.C. Cir. 1989) ("The state secrets privilege is a common law evidentiary rule . . . .").

also City of Milwaukee v. Illinois & Michigan, 451 U.S. 304, 313–15 (1981) ("We have always recognized that federal common law is subject to the paramount authority of Congress. It is resorted to [i]n absence of an applicable Act of Congress . . . . Thus the question [is] whether the legislative scheme '[speaks] directly to a question.'"); *County of Oneida v. Oneida Indian Nation*, 470 U.S. 226, 236–37 (1985).[4] That is clearly the case here. The plain language of Section 1806(f) speaks directly to the procedures applicable to the discovery Wikimedia seeks. FISA's text and legislative history manifest a clear expression of congressional intent to displace the common law in this area.

To begin, Section 1806(f) is deliberately broad in scope and mandatory in application. The statute makes clear that it applies universally "whenever *any* motion or request is made . . . pursuant to *any* . . . *statute or rule* of the United States" to "discover" information relating to FISA surveillance. 50 U.S.C. § 1806(f) (emphasis added); *see also* S. Rep. No. 95-604, pt.1, at 57 ("The Committee wishes to make very clear that the procedures set out in [subsection 1806(f)] apply whatever the underlying rule or statute referred to in [a party's] motion. This is necessary to prevent the carefully drawn procedures in [section 1806(f)] from being bypassed[.]"). The statute applies to efforts to discover all "materials relating to electronic surveillance," "notwithstanding any other law." 50 U.S.C. § 1806(f); *see also* 18 U.S.C. § 2712(b) ("Notwithstanding any other provision of law, [§ 1806(f)] shall be the exclusive means by which materials governed by those sections may be reviewed."). And the statute makes its

[4] *See also* Fed. R. Evid. 501 ("The common law—as interpreted by United States courts in the light of reason and experience—governs a claim of privilege unless any of the following provides otherwise: the United States Constitution; a federal statute; or rules prescribed by the Supreme Court.").

discovery procedures mandatory. 50 U.S.C. § 1806(f) ("the United States district court . . . *shall* . . . review" (emphasis added)).

For discovery efforts that fall within Section 1806(f)'s broad scope, FISA provides a comprehensive regime regulating access to information regarding the lawfulness of electronic surveillance. As explained above, FISA gives the government two choices in responding to discovery requests for information relating to electronic surveillance under FISA. If the Attorney General files an affidavit stating that the disclosure sought would "harm the national security of the United States," then FISA provides for in camera and ex parte review of the government's discovery responses, as well as the possibility of disclosure to the movant. *Id.* If the Attorney General does not file such an affidavit, then the government must disclose the material sought to the requester. *Id.*

The plain meaning of FISA thus displaces the state secrets privilege with regard to the discovery of information "relating to electronic surveillance." *Id.*

The legislative history reinforces Congress's preclusive intent. Congress's express purpose in enacting FISA was "to curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it." S. Rep. No. 95-604, pt. 1, at 8; *see, e.g.*, H.R. Rep. No. 95-1283, pt. 1, at 101 (1978) (FISA "prohibit[s] the President, notwithstanding any inherent powers, from violating the terms of that legislation"); S. Rep. No. 95-604, pt. 1, at 64 (FISA "puts to rest the notion that Congress recognizes an inherent Presidential power to conduct such surveillances in the United States outside of the procedures contained in [FISA and Title III]"); *id*. at 6 ("[T]he bill recognizes no inherent power of the President in this area.").

In enacting FISA, Congress intended to occupy the field of foreign intelligence electronic surveillance, stating unequivocally that the "procedures in . . . [FISA and related statutes] shall be the exclusive means by which electronic surveillance, as defined in [FISA] . . . may be conducted." 18 U.S.C. § 2511(2)(f); H.R. Rep. No. 95-1720, at 35 (invoking *Youngstown Sheet and Tube Co. v. Sawyer*, 343 U.S. 579 (1952), so as to make clear congressional intent to occupy the field of foreign intelligence surveillance contrary to any invocation of Executive authority). Congress reconfirmed that exclusivity when it enacted the FISA Amendments Act of 2008. 50 U.S.C. § 1812. As the Department of Justice has previously conceded, Congress's "overriding purpose" in enacting FISA was to "bring[] the use of electronic surveillance under congressional control." U.S. Dep't of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President*, at 20 (Jan. 19, 2006). FISA was thus meant to "represent the sole authority for national security electronic surveillance" to "insure[] executive accountability." 124 Cong. Rec. S10,903–04 (daily ed. Apr. 20, 1978).

In short, FISA regulates electronic surveillance, including the discovery Wikimedia seeks. The government may avoid FISA's statutory discovery provision only by taking the radical position that FISA is itself unconstitutional, based on a raw assertion of executive power that overrides Congress's power. That is, the government must argue that FISA is unconstitutional under Article II of the Constitution. The executive's power under Article II is at its "lowest ebb," however, when the executive acts in direct contravention of a congressional mandate. *See, e.g.*, *Youngstown*, 343 U.S. at 637–38 (Jackson, J., concurring); *cf. Japan Whaling Ass'n v. Am. Cetacean Soc'y*, 478 U.S. 221, 233 (1986) (an agency "may not act contrary to the will of Congress when exercised within the bounds of the Constitution. . . . [I]f the intent of Congress is clear, that is the end of the matter."). "Courts can sustain exclusive Presidential

control in such a case only by disabling the Congress from acting upon the subject." *Youngstown*, 343 U.S. at 637–38. The Supreme Court has theorized about the possibility of such a power, but it has never recognized one in fact. There are many reasons this Court should not do so here.

First, Congress clearly has the authority to regulate foreign intelligence surveillance on U.S. soil, particularly when it implicates U.S. individuals, as in this case. That broader authority encompasses the authority to require the government to disclose information—to the Court or, in appropriate circumstances and with appropriate protections, to a party's counsel—in the defense of that surveillance. Indeed, Congress has regulated foreign intelligence surveillance on U.S. soil for 40 years, and the government cannot credibly claim that FISA is unconstitutional for doing so. Nor can it credibly argue that FISA or its discovery provision is unconstitutional on the ground that it requires the government to disclose extremely sensitive information to Article III courts. The government routinely discloses such information to the FISC to justify this surveillance, and to other Article III courts when evidence acquired as a result of that surveillance is used in criminal trials.

Second, Congress and the courts have a long-established and constitutional role to play in the handling of sensitive and classified information. Congress regulates classified information in many contexts. For example, Title 50 of the U.S. Code regulates national security information and requires the Executive Branch to disclose such information—including illegal intelligence activity—to congressional committees. *See* 50 U.S.C. §§ 3091, 3125, 3345, 3365; *see also* 42 U.S.C. §§ 2162–2169 (nuclear data). Congress has also directed the President to establish certain procedures governing access to classified material, 50 U.S.C. §§ 3161–3164; *see also id.* §§ 831–835 (personnel security procedures for the NSA), and it has mandated that, in so doing,

the President must provide due process, *id.* § 3161(a). And of course Congress enacted the Classified Information Procedures Act to regulate the use of classified information in criminal proceedings. *See* 18 U.S.C. app. 3 §§ 1–16. "Congressional regulation of the use of classified information by the executive branch through FISA and other statutes is therefore well-established." *In re NSA Telecomms. Records Litig.*, 564 F. Supp. 2d 1109, 1122 (N.D. Cal. 2008).

The courts have also long had a hand in regulating Executive Branch classification. Courts are routinely called upon to decide under the Freedom of Information Act whether information sought by requesters is "properly classified." *See* 5 U.S.C. § 552(b)(1). Courts perform an even more robust review of Executive Branch secrecy when members of the public assert a First Amendment right of access to judicial records that contain classified information. *See, e.g.*, *In re Wash. Post Co.*, 807 F.2d 383, 390–92 (4th Cir. 1986). And for the last forty years under FISA and the Classified Information Procedures Act, courts have regularly reviewed FISA or other classified material relevant to criminal prosecutions to make case-by-case determinations of whether to order the government to disclose portions of that material to defendants or their counsel. *See* 50 U.S.C. § 1806(f); 18 U.S.C. app. 3 §§ 4, 6, 8; *see, e.g.*, *United States v. Rosen*, 447 F. Supp. 2d 538, 545 (E.D. Va. 2006) (Ellis, J.) ("[T]he FISA dockets were reviewed *de novo* . . . . Importantly, the review was both searching and conducted with special care . . . .").

Third, FISA's discovery provision accommodates the government's interests. It permits the government to withhold discovery from a party if—akin to the process required to invoke the state secrets privilege—the Attorney General attests to the harm that would flow from that disclosure. *See* 50 U.S.C. § 1806(f). FISA requires the government to disclose discovery material

sought to the Court, but that disclosure is no more extensive than the FISC itself requires or could require of the government in deciding whether to approve the government's surveillance in the first instance. *See, e.g.*, 50 U.S.C. § 1804 (required contents of FISA application); *id.* § 1881a (same for Section 702 of FISA); *see also* [*Redacted*], 2011 WL 10945618, at *2 (noting that the FISC "directed the government to answer a number of questions in writing" concerning compliance violations).

Fourth, and finally, it would raise serious constitutional questions for the Court to override the mechanism that Congress has chosen for the protection of individual rights from overreaching executive surveillance. The balance Congress has implemented—by permitting the government to conduct foreign intelligence surveillance on U.S. soil, while subjecting that surveillance to judicial oversight—is a deliberate one. This Court should not disturb it in favor of a common law privilege devised by courts without the institutional competence that Congress possesses to balance the competing interests involved. *Cf. Youngstown*, 343 U.S. at 638 ("Presidential claim to a power at once so conclusive and preclusive must be scrutinized with caution, for what is at stake is the equilibrium established by our constitutional system.").

For these reasons, FISA's discovery procedures displace the state secrets privilege with respect to the discovery sought by Wikimedia. The only two courts to have directly addressed this question have agreed that FISA's plain language and legislative history are "enough, certainly, to establish that it preempts the state secrets privilege as to matters to which it relates." *In re NSA Telecomms. Records Litig.*, 564 F. Supp. 2d at 1119; *see also id.* at 1119–23; *Jewel v. NSA*, 965 F. Supp. 2d 1090, 1104–05 (N.D. Cal. 2013). As one of the courts noted, "[i]t is clear Congress intended for FISA to displace federal common law rules such as the state secrets privilege with regard to matters within FISA's purview." *Id.* at 1105–06; *see also In re*

NSA Telecomms. Records Litig., 564 F. Supp. 2d at 1119–20 (finding that the "legislative history is evidence of Congressional intent that FISA should displace federal common law rules such as the state secrets privilege with regard to matters within FISA's purview").

In FISA, Congress laid down specific, comprehensive, and mandatory procedures for courts to employ when the lawfulness of electronic surveillance under FISA is challenged. Those statutory discovery procedures, not the state secrets privilege, apply here.

C. Even if it applied, the state secrets privilege would not bar disclosure of the information Wikimedia seeks.

Even if FISA did not displace the state secrets privilege, the privilege would not bar the discovery Wikimedia seeks. The state secrets privilege, if it is to apply, "must be asserted by [the government]" and "is not to be lightly invoked." *Reynolds*, 345 U.S. at 7. "There must be formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer." *Id.* at 7–8; *Abilt v. CIA*, 848 F.3d 305, 311 (4th Cir. 2017). "The claim also must be presented in sufficient detail for the court to make an independent determination of the validity of the claim of privilege and the scope of the evidence subject to the privilege." *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1080 (9th Cir. 2010).

Because the head of the NSA has not formally invoked the state secrets privilege, the privilege is not yet in issue. Wikimedia will reply to any invocation of it at the appropriate time, but Plaintiff notes now that even if the government invokes the privilege in response to this motion, the privilege would not apply because disclosure of the information Wikimedia seeks would not harm national security.[5] Plaintiff makes two brief points at this stage.

[5] Indeed, even were the government to properly invoke the privilege, the Court would then analyze whether and to what extent the privilege applies after the appropriate balancing. *See,*

First, disclosure of the fact that the NSA has reviewed at least one of Wikimedia's communications in the course of Upstream surveillance could not possibly endanger national security. If the government were to disclose as much, it would be acknowledging three facts, none of which is sensitive or would risk harm to national security: (1) The government would be acknowledging that Upstream surveillance involves the review of Internet communications, but the government has already acknowledged as much. (2) The government would be acknowledging that Upstream surveillance involves the review of the sort of Internet communications that Wikimedia engages in—namely, "web activity"—but the government has acknowledged that fact, too. *See* June 1, 2011 FISC Submission at 30 (Toomey Decl., Ex. 25). (3) The government would be acknowledging that Wikimedia's web traffic traverses at least one of the Internet backbone circuits on which the NSA conducts Upstream surveillance. But given the ubiquity of Wikimedia's web traffic as it communicates with hundreds of millions of individuals around the world, and the unpredictable nature of Internet routing, that would reveal nothing about which circuits the NSA is monitoring. To confirm that the NSA has reviewed one of Wikimedia's communications would reveal as much as confirming that an NYPD officer saw a yellow taxi cab while patrolling the streets of New York. It would reveal nothing about the identity of the NSA's many targets. It would reveal nothing about the location of the NSA's surveillance devices. And it would reveal nothing that would allow the NSA's targets to evade Upstream surveillance.

---

e.g., *Abilt*, 848 F.3d at 311–12. Whenever possible, sensitive information must also be disentangled from non-sensitive information to allow for the release of the latter. *Ellsberg v. Mitchell*, 709 F.2d 51, 52–53 (D.C. Cir. 1983); *see, e.g.*, *DTM Research, LLC v. AT&T Corp.*, 245 F.3d 327, 334 (4th Cir. 2001).

Second, no harm could come from requiring the government to disclose other information Plaintiff seeks, given the close relationship between that information and the government's extensive public disclosures concerning the operation of Upstream surveillance. For example, Wikimedia asked Defendants to describe their understanding of the definition of the term "circuit"—a term that the Privacy and Civil Liberties Oversight Board used when explaining that Upstream surveillance entails the monitoring of communications as they transit telecommunications "circuits" on the Internet backbone. PCLOB Report at 36–37. Yet Defendants provided only a generic and vague description of "circuit," while withholding responsive information. *See* NSA Resp. to Pl. Interrogatory No. 2 (Toomey Decl., Ex. 11). Defendants refused even to admit that Upstream surveillance occurs at multiple circuits on the Internet backbone—notwithstanding the PCLOB's discussion of how Upstream surveillance takes place on "circuits" (plural) with the compelled assistance of telecommunications "providers" (plural). *See* PCLOB Report at 35; Pl. Request for Admission No. 13 (Toomey Decl., Ex. 1); NSA Resp. to Pl. Request for Admission No. 13 (Toomey Decl., Ex. 9). Admitting this fact—when it has already been admitted in the PCLOB Report, a document that Defendants reviewed and declassified—could not conceivably cause harm to national security. PCLOB Report at 3–4.

Similarly, Defendants provided non-responsive answers (or no answers at all) to Wikimedia's requests for information about the defining features of "Internet transactions" and the meaning of "discrete communication"—technical terms that Defendants and the FISC use over and over to describe the basic units of Internet traffic subject to Upstream surveillance. *See* Pl. Interrogatories No. 6–8 (Toomey Decl., Ex. 1); June 1, 2011 FISC Submission (Toomey Decl., Ex. 25); [*Redacted*], 2011 WL 10945618; NSA Resp. to Pl. Interrogatories No. 6–8

(Toomey Decl., Ex. 11) (Rog. 6: "Describe your understanding of the definition of the term 'discrete communication' . . . ."; Resp. to Rog. 6: "[T]he term 'discrete communication' means a single communication."). When Plaintiff asked similar questions about the terms "screen," "scanned," and "filtering mechanism"—which Defendants have used publicly and in their discovery responses to describe how the NSA's surveillance devices examine intercepted Internet traffic—Defendants simply provided a set of circular responses. *See* NSA Resp. to Pl. Interrogatories No. 3–5 (Toomey Decl., Ex. 11) (Rog. 5: "Describe your understanding of the word 'screen'"; Resp. to Rog. 5 ". . . 'screen' . . . meant . . . the use of a screening device"). Defendants have even refused to disclose portions of documents stating that Upstream surveillance is conducted at international Internet links, even though that fact is officially disclosed in a FISC opinion. *Compare* [*Redacted*], 2011 WL 10945618, at *15, *with* June 1, 2011 FISC Submission at 29 (Toomey Decl., Ex. 25).

Finally, the government has refused to admit that the NSA screens the contents of Internet web traffic—that is, HTTP and HTTPS traffic. *See* Pl. Requests for Admission No. 37, 38 (Toomey Decl., Ex. 1). Yet the government has publicly acknowledged Upstream collection of "web activity," *see* June 1, 2011 FISC Submission at 30, and it has acknowledged screening the contents of communications in order to identify those it wishes to retain, *see* PCLOB Report at 36–37. These government disclosures are an admission that Upstream surveillance involves screening the contents of Internet web traffic, and so Defendants' apparent belief that responding to Wikimedia's request would harm national security is unjustified.

D. Section 3024(i) does not establish a litigation privilege.

The government has defended many of its refusals to respond to Wikimedia's discovery requests by invoking a provision of the National Security Act, 50 U.S.C. § 3024(i), but that provision is simply not a litigation privilege. Section 3024(i)(1) provides:

> The Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.

By its plain terms, this provision has nothing to do with discovery. It does not authorize the Director of National Intelligence to withhold otherwise discoverable information either from a plaintiff or a federal court—let alone information relating to whether electronic surveillance is unauthorized or unconstitutional. *See generally Webster v. Doe*, 486 U.S. 592, 600–05 (1988) (rejecting claim that related section of the National Security Act, Section 3023, bars judicial review or discovery related to constitutional claims). Instead, it directs the Director of National Intelligence to safeguard sensitive information. There are countless statutes that similarly direct various executive officials to safeguard sensitive information, but Wikimedia is not aware of any case law suggesting that such commonplace decrees establish litigation privileges.

In other cases, the government has argued that Section 3024(i) is a litigation privilege because it has been held to be an exemption statute under the Freedom of Information Act, *see, e.g.*, *CIA v. Sims*, 471 U.S. 159 (1985), but that does not follow. FOIA's exemptions do not establish freestanding litigation privileges. They exempt agency records from the general disclosure requirement imposed *by FOIA*. *See* 5 U.S.C. § 552(b)(3). But Wikimedia does not seek to compel disclosure under FOIA, and therefore a statute defining FOIA's reach simply has no bearing on the reach of discovery here.

In any event, even if Section 3024(i) established a general discovery privilege, FISA's more specific discovery provision, 50 U.S.C. § 1806(f), would control discovery in this case under ordinary principles of statutory interpretation. *Green v. Bock Laundry Mach. Co*., 490 U.S. 504, 524–26 (1989) ("A general statutory rule usually does not govern unless there is no more specific rule."); *Crawford Fitting Co. v. J. T. Gibbons, Inc.*, 482 U.S. 437, 444–45 (1987).

E. Section 3605(a) is not a bar to discovery in this case.

The government has defended many of its refusals to respond to Plaintiff's discovery requests in reliance on Section 6 of the NSAA, 50 U.S.C. § 3605(a), but this reliance is also misplaced. Section 3605 reads in relevant part:

> [N]othing in this chapter or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, or any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such agency.

The government appears to interpret Section 3605 as a general bar on compelled disclosure of almost any information in the NSA's possession. As with Section 3024(i), whatever the meaning of the general language of Section 3605, FISA's more specific and later-enacted discovery provision supersedes it in this case. *See Green*, 490 U.S. at 524. FISA requires the disclosure to this Court—and, if necessary, to Plaintiff—of discovery relevant to Wikimedia's challenge to the lawfulness of the NSA's electronic surveillance of Wikimedia's communications. 50 U.S.C. § 1806(f). That specific requirement trumps the more general language of Section 3605.

There is, moreover, a fatal paradox in the government's broad interpretation of Section 3605. If Section 3605 truly barred the compelled disclosures the government believes it to bar, then Section 3605 would throw into disarray all of FISA, not just FISA's discovery provision. FISA, after all, requires the NSA to disclose a substantial amount of technical and other information in seeking targeted surveillance orders, *see* 50 U.S.C. § 1804; in seeking the year-long surveillance orders at issue in this case, *see id.* § 1881a; and in defending the lawfulness of admitting the fruits of that surveillance at a criminal trial, *see id.* § 1806(f). And to facilitate oversight, FISA requires the government to make periodic disclosures to the FISC and to Congress, *id.* § 1881a(m), and the FISC often orders the government to make supplemental disclosures concerning compliance violations, *see, e.g.*, [*Redacted*], 2011 WL 10945618, at *2. If

the government's apparent interpretation of Section 3605 were correct, then all of these disclosures could not in fact be compelled, and FISA's complex and interwoven scheme would be undone. The simple solution to this paradox is the one required by the familiar canon that requires courts to give effect to specific statutory commands over general ones.

In any event, Section 3605 does not have the broad meaning the government appears to believe it does. Section 3605 was enacted at the request of President Eisenhower's Department of Defense ("DOD"), five years after a presidential directive created the NSA itself. The statute was adopted with the express, limited intent of preventing the NSA from having to disclose its personnel information to the Civil Service Commission. S. Rep. No. 86-284, pt.1, at 2-3 (1959) ("The purpose of this legislation is to eliminate an administrative dilemma in which the National Security Agency and the Civil Service Commission find themselves by exempting the former from the provisions of the Classification Act of 1949, as amended."). Disclosing personnel information to the Civil Service Commission, the DOD argued in advocating for the statute, would not be practicable in light of security considerations. *See* Letter from Donald A. Quarles, Acting Secretary of Def., to Richard M. Nixon, President of the Senate (Jan. 2, 1959), *included in* S. Rep. No. 86-284, pt. 1, at 3 (1959). In other words, Section 3605 is a statute narrowly aimed at protecting the NSA's personnel records. The statute's use of terms such as "organization," "function," and "activities" must be understood in that context.

Many courts have recognized the havoc that would be wrought by interpreting Section 3605 too broadly. A district court in an action regarding AT&T's cooperation with the NSA's post-9/11 surveillance expressed that concern:

> [If] section 6 is taken to its to its logical conclusion, it would allow the federal government to conceal information regarding blatantly illegal or unconstitutional activities simply by assigning these activities to the NSA or claiming they implicated information about

> the NSA's functions. In short, the Court is hard-pressed to read section 6 as essentially trumping every other Congressional enactment and Constitutional provision. Indeed, at oral argument, the government agreed that there is likely a limit to its ability to invoke section 6, though it balked at defining where the line would be drawn, insisting that wherever the line is, this case falls squarely inside it. The Court is skeptical that section 6 is properly read as broadly as the government urges.

Terkel v. AT&T Corp., 441 F. Supp. 2d 899, 905 (N.D. Ill. 2006). Even in the context of FOIA, in which the NSA has many options for withholding information concerning its surveillance operations, courts have recognized the "potential for [an] unduly broad construction" of Section 3605. *Founding Church of Scientology v. NSA*, 610 F.2d 824, 828–29 (D.C. Cir. 1979) ("[A] term so elastic as 'activities' should be construed with sensitivity to the hazard(s) that Congress foresaw. . . . [C]ourts must be particularly careful when scrutinizing claims of exemptions based on such expansive terms.").

The Court need not resolve the dispute over the breadth of Section 3605, however. It is sufficient in this case to recognize that FISA's discovery provision supersedes Section 3605, whatever the latter's meaning. Accordingly, Section 3605 does not bar the discovery Plaintiff seeks.

III. Other objections asserted by Defendants

Defendants have asserted various other objections to the requests at issue in this motion. Plaintiff addresses those objections below only insofar as Defendants indicated during the parties' meet and confers that they would rely on an objection even if their state secrets and related claims were rejected. For many of these requests, Defendants' continued objections are puzzling because they have, in fact, provided responsive information so long as it was unclassified. Insofar as Defendants' true objection is state secrets, the Court's analysis should begin and end there.

A. Relevance objections

Defendants have objected that certain of Wikimedia's requests are irrelevant to the question of whether Wikimedia's communications are intercepted, copied, or reviewed in the course of Upstream surveillance, and are therefore beyond the scope of jurisdictional discovery. Wikimedia's requests, however, are unquestionably relevant to that issue.

1. *Requests seeking the definition or meaning of key terms related to Upstream surveillance*

   - Pl. Interrogatories No. 6, 8

Wikimedia has sought basic information concerning the definition, meaning, or characteristics of key terms the government has used to publicly describe Upstream surveillance and the Internet communications subject to that surveillance. Those key terms include what the NSA calls "discrete communications," "single communication transactions," and "multi-communication transactions." Defendants contend that these requests are not relevant, but they plainly are. These requests bear on Wikimedia's showing of how Upstream surveillance results in the copying and review of Wikimedia's communications as they transit the Internet backbone. Defendants, the FISC, and the PCLOB have repeatedly used these terms to describe the basic units of Internet traffic subject to Upstream surveillance. *See, e.g.*, June 1, 2011 FISC Submission (Toomey Decl., Ex. 25); [*Redacted*], 2011 WL 10945618, at *1–3, *9–30. Indeed, as the government was forced to acknowledge to the FISC in 2011, any accurate description of how Upstream surveillance operates requires an understanding of these terms in relation to

communication over the Internet. *See id.* at *1–3, *9–13; June 1, 2011 FISC Submission at 1–12, 21–22, 30–32 & n.1 (Toomey Decl., Ex. 25).[6]

2. *Requests seeking FISC opinions and orders, FISC submissions, and targeting procedures related to Upstream surveillance*

- Pl. Requests for Production No. 18, 21–22
- Pl. Requests for Admission No. 28–30

Defendants have also objected on relevance grounds to Wikimedia's requests for FISC opinions and orders, FISC submissions, and targeting procedures related to Upstream surveillance. As the public record shows, however, these documents broadly and variously describe how and where Upstream surveillance is conducted, including: the ways in which the NSA's surveillance devices examine Internet communications intercepted in the course of Upstream surveillance; the breadth of Upstream surveillance, in terms of the volume of communications and the comprehensiveness of the NSA's searches; the kinds of linkage points on the Internet backbone where Upstream surveillance takes place; the types of Internet communications that are subject to Upstream surveillance; the characteristics of "Internet transactions" and "Internet communications" as the NSA uses those terms; and the ways in which the NSA overcollects Internet communications based on the surveillance devices it uses. *See, e.g.*, [*Redacted*], 2011 WL 10945618, at *1–3, *9–28; June 1, 2011 FISC Submission at 1–12, 21–22, 30–32, 38–41 & n.1 (Toomey Decl., Ex. 25); 2009 NSA Targeting Procedures, Ex. E to Pl. Requests for Admission (Toomey Decl., Ex. 2) (describing how the NSA targets "Internet links that terminate in a foreign country").

[6] Notably, Defendants did not object on relevance grounds to Plaintiff's Interrogatory No. 7, which sought very similar information about "Internet transactions." *See* NSA Resp. to Pl. Interrogatory No. 7 (Toomey Decl., Ex. 11).

3. *Requests addressing the processing and retention of Internet communications in the course of Upstream surveillance*

- Pl. Interrogatories No. 14–15
- Pl. Request for Production No. 10

Wikimedia has sought information about the ways in which the NSA accesses the contents of Internet communications pursuant to Upstream surveillance, and the overall volume of communications the NSA retains as a consequence of those processes. This information bears on Wikimedia's showing that Upstream surveillance involves the bulk copying and review of Internet communications, and it helps establish a lower bound in terms of the number of communications subject to Upstream surveillance each year. *See* PCLOB Report at 37, 111 n.476 (stating that the NSA retained 26.5 million Internet transactions in 2011, while acknowledging that Upstream surveillance "may require access to a larger body of international communications"); *id.* at 7–10, 22, 32–33, 35–41 & n.157, 79, 119–26, 143–45.

4. *Requests seeking authentication of NSA documents*

- Pl. Requests for Admission No. 16–21, 25–30

Defendants objected on relevance grounds to Wikimedia's requests concerning the authenticity and authoritativeness of several NSA documents. Even a passing review of these documents shows that they relate to the NSA's surveillance of Wikimedia's communications, the fact that the NSA is conducting Upstream surveillance at Internet backbone chokepoints, and the large number of Internet circuits the NSA is monitoring at those chokepoints. *See* NSA Resp. to Pl. Requests for Admission No. 16–21, 25–30 (Toomey Decl., Ex. 9).

5. *Objection based on date-range*

- Pl. Requests for Production No. 10, 13–16, 18, 21–24

Defendants have objected that certain requests are irrelevant and/or burdensome because they seek documents spanning a number of years during which Upstream surveillance has

operated. *See* NSA Resp. to Pl. Requests for Production (Toomey Decl., Ex. 13). In response, Wikimedia narrowed several of its requests, *see* Toomey Decl., Ex. 1, and offered to negotiate over others to mitigate any unreasonable burden claimed by Defendants. In a handful of instances, Wikimedia continues to seek documents that date back to the initiation of this surveillance program—including any Wikimedia communications that Defendants possess by virtue of Upstream surveillance. The fact that the NSA intercepted some of Wikimedia's trillions of communications in the past, as they transited the Internet backbone, is clearly relevant to the question of whether the NSA has continued to do so. *See* Pl. Requests for Production 23–24 (Toomey Decl., Ex. 1). Moreover, Defendants' burden objections are unjustified. Although Wikimedia provided Defendants with information to facilitate a search for these records, Defendants have not even attempted to undertake such a search. Wikimedia's requests for foundational documents—such as early FISC opinions, or NSA targeting procedures showing that Upstream surveillance is conducted at "Internet links that terminate in a foreign country"—also offer relevant evidence about the basic infrastructure of this surveillance program. These requests, as narrowed by Wikimedia, can be produced without unreasonable burden. *See* Toomey Decl., Ex. 1.

B. Objection to Requests for Admissions

- Pl. Requests for Admission No. 6–10, 13–15

Defendants object that some of Wikimedia's Requests for Admission are improper on the ground that such requests should not be used as "discovery devices." *See, e.g.*, NSA Resp. to Pl. Requests for Admission Nos. 6–10, 13–15 (Toomey Decl., Ex. 9). This objection is misplaced. As an initial matter, based on the plain text of Rule 36 and its placement within Title V of the Federal Rules of Civil Procedure, there is no question that requests for admission are discovery tools. *See* Fed. R. Civ. P. 36(a) ("A party may serve on any other party a written request to

admit . . . the truth of any matters within the scope of Rule 26(b)(1)" relating to "facts, the application of law to fact, or opinions about either," and "the genuineness of any described documents."); *Jackson v. Washington Metro. Area Transit Auth.*, No. WGC-16-1050, 2016 WL 6569062, at *5 (D. Md. Nov. 4, 2016). Insofar as Defendants' objection is based on the theory that requests for admission "presuppose that the propounding party knows or believes the facts sought," *James v. Maguire Corr. Facility*, No. C 10-1795 SI, 2012 WL 3939343, at *4 (N.D. Cal. Sept. 10, 2012), that is precisely the case here. Wikimedia has sought admissions concerning information that it knows or believes to be true. *See, e.g.*, Pl. Request for Admission No. 6 (Toomey Decl., Ex. 1) ("Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS . . . ."); Pl. Request for Admission No. 13 ("Admit that the NSA conducts Upstream surveillance on multiple INTERNET BACKBONE CIRCUITS.").

Not only were Defendants' objections to Wikimedia's Requests for Admissions unwarranted, but their responses were improper as well. Rather than clearly admit, deny, or explain their failure to admit or deny Wikimedia's requests, as required by Rule 36, Defendants provided "responses" that essentially recast the requests in Defendants' chosen terms. *See, e.g.*, NSA Resp. to Pl. Request for Admission No. 8 (Toomey Decl., Ex. 9) (in response to a request for admission concerning bulk review of communications, NSA stated that communications are filtered and screened); NSA Resp. to Pl. Request for Admission No. 10 (Toomey Decl., Ex. 9) (in response to a request for admission concerning the review of communications, NSA stated that communications are filtered and screened). These non-responsive answers fail to satisfy Rule 36. *See, e.g.*, *Turner v. California Forensic Med. Grp.*, No. 09-cv-3040-GEB-CMK-P, 2013 WL 1281785, at *3 (E.D. Cal. Mar. 26, 2013) ("Plaintiff may either admit, deny, or object to the

request as it is written. He may not alter the request or rewrite it in order to admit to something that was not asked."); *Warren v. Sessoms & Rogers, P.A.*, No. 09-cv-00159-BO, 2012 WL 13024154, at *5 (E.D.N.C. Nov. 26, 2012) ("Gamesmanship, non-responsive answers, or evasiveness in response to a request for admission warrant a court deeming the matters admitted.").

IV. Deposition testimony

Defendant NSA has agreed to provide a witness in response to certain topics identified in Plaintiff's Notice of Deposition Pursuant to Rule 30(b)(6). *See* Toomey Decl., Ex. 24. Nonetheless, the NSA has objected to each topic insofar as Wikimedia seeks information that the NSA claims is protected by the state secrets privilege, 50 U.S.C. § 3024(i), and 50 U.S.C. § 3605(a). *See* Toomey Decl., Ex. 24. However, for the reasons discussed above, the state secrets privilege is displaced by FISA and the cited statutes are inapplicable. *See* Section II *supra*. Moreover, virtually all of Wikimedia's deposition topics encompass facts that the government has publicly disclosed in its FISC submissions, FISC opinions, the PCLOB Report, and official statements—and thus claims of secrecy are not a valid reason for the NSA to refuse to provide testimony concerning many of the facts at issue.

For these reasons, Wikimedia requests that the Court apply the in camera review procedures in 50 U.S.C. § 1806(f) to resolve, in an orderly fashion, any disputes arising out of the NSA deposition. In particular, to the extent the NSA refuses to provide a response to any deposition question based on a claim that the response is classified, Wikimedia requests that the Court order the following:

(1) Within two weeks of the Court's ruling on this issue, Wikimedia shall file with the Court a motion to compel that identifies from the deposition transcript any questions for which

Wikimedia seeks to compel answers over the NSA's objection that the information is protected by the state secrets privilege, 50 U.S.C. § 3024(i), and/or 50 U.S.C. § 3605(a).

(2) Within two weeks of Wikimedia's filing and serving the motion to compel, the NSA shall submit for in camera review answers to the questions in the form of written responses and/or live oral testimony.

Conclusion

For the foregoing reasons, pursuant to FISA's discovery procedures, 50 U.S.C. § 1806(f), the Court should order Defendants to provide the requested discovery responses and deposition testimony for its in camera review. If the Court concludes that any of the withheld information has already been officially disclosed, or that its disclosure to Wikimedia would not harm national security, the Court should order disclosure of the information to Wikimedia. In any event, pursuant to 50 U.S.C. § 1806(f), the Court should order disclosure to Wikimedia of any withheld information, under appropriate security procedures and protective orders, where such disclosure is "necessary" to resolve the factual and legal questions at issue.

Dated: March 26, 2018

Respectfully submitted,

/s/
Deborah A. Jeon (Bar No. 06905)
David R. Rocah (Bar No. 27315)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838
jeon@aclu-md.org

/s/
Patrick Toomey (pro hac vice)
(*signed by Patrick Toomey with permission of Deborah A. Jeon*)
Ashley Gorski (pro hac vice)
Jonathan Hafetz (pro hac vice)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ptoomey@aclu.org

Alex Abdo (pro hac vice)
Jameel Jaffer (pro hac vice)
KNIGHT FIRST AMENDMENT INSTITUTE
AT COLUMBIA UNIVERSITY
475 Riverside Drive, Suite 302
New York, NY 10115
Phone: (646) 745-8500
alex.abdo@knightcolumbia.org

Counsel for Plaintiff